AMENDMENTS TO THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for scanning data, comprising:

a) executing scanning control logic utilizing a central processing unit;

b) identifying a request related to data at the central processing unit;

c) indicating a location of the data to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic;

d) waiting for results from the scanning co-processor;

e) executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor; and

f) initiating an event based on the results from the scanning co-processor;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data;

wherein the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria;

wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor;

wherein the scanning co-processor is capable of performing an additional scan on the additional data while scanning the data;

wherein the location of the data indicated to the scanning co-processor includes a memory location of the data stored in memory, where the memory is separate from and coupled to the scanning co-processor and the central processing unit via a bus that employs direct memory access.

2. (Previously Presented) The method as recited in claim 1, and further comprising processing the data utilizing the central processing unit upon the receipt of

favorable results from the scanning co-processor including a situation where malicious code is not detected.

3. (Currently Amended) The method as recited in claim 1, wherein the central processing unit is coupled to the scanning co-processor via [[a]]the bus.

4. (Original) The method as recited in claim 1, wherein the scanning control logic includes hardware.

5. (Original) The method as recited in claim 3, wherein the scanning control logic is stored on the scanning co-processor.

6. (Original) The method as recited in claim 1, wherein the scanning control logic includes software.

7. (Currently Amended) The method as recited in claim 6, wherein the scanning control logic is stored in the memory.

8. (Original) The method as recited in claim 1, wherein the event is initiated under the control of the scanning control logic.

9. (Original) The method as recited in claim 1, wherein the scanning co-processor performs content scanning.

10. (Original) The method as recited in claim 1, wherein the scanning co-processor performs virus scanning.

11. (Currently Amended) The method as recited in claim 1, wherein the scanning co-processor includes additional memory.

12. (Currently Amended) The method as recited in claim 11, wherein virus signatures are stored in the additional memory.

13. (Currently Amended) The method as recited in claim 11, wherein rule sets are stored in the additional memory.

14. (Cancelled)

15. (Cancelled)

16. (Cancelled)

17. (Currently Amended) A computer program product for scanning data, comprising:

a) computer code for executing scanning control logic utilizing a central processing unit;

b) computer code for identifying a request related to data at the central processing unit;

c) computer code for indicating a location of the data to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic;

d) computer code for waiting for results from the scanning co-processor;

e) computer code for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor; and

f) computer code for initiating an event based on the results from the scanning co-processor;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data;

wherein the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria;

wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor;
wherein the scanning co-processor is capable of performing an additional scan on the additional data while scanning the data;
wherein the location of the data indicated to the scanning co-processor includes a memory location of the data stored in memory, where the memory is separate from and coupled to the scanning co-processor and the central processing unit via a bus that employs direct memory access.

18. (Previously Presented) The computer program product as recited in claim 17, and further comprising computer code for processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected.

19. (Currently Amended) The computer program product as recited in claim 17, wherein the central processing unit is coupled to the scanning co-processor via [[a]]the bus.

20. (Original) The computer program product as recited in claim 17, wherein the scanning control logic includes hardware.

21. (Original) The computer program product as recited in claim 20, wherein the scanning control logic is stored on the scanning co-processor.

22. (Original) The computer program product as recited in claim 17, wherein the scanning control logic includes software.

23. (Currently Amended) The computer program product as recited in claim 22, wherein the scanning control logic is stored in the memory.

24. (Original) The computer program product as recited in claim 17, wherein the event is initiated under the control of the scanning control logic.

25. (Original) The computer program product as recited in claim 17, wherein the scanning co-processor performs content scanning.

26. (Original) The computer program product as recited in claim 17, wherein the scanning co-processor performs virus scanning.

27. (Currently Amended) The computer program product as recited in claim 17, wherein the scanning co-processor includes additional memory.

28. (Currently Amended) The computer program product as recited in claim 27, wherein virus signatures are stored in the additional memory.

29. (Currently Amended) The computer program product as recited in claim 27, wherein rule sets are stored in the additional memory.

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Currently Amended) A system for scanning data, comprising:

a) logic for executing scanning control logic utilizing a central processing unit;

b) logic for identifying a request related to data at the central processing unit;

c) logic for indicating a location of the data to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic;

d) logic for waiting for results from the scanning co-processor;

e) logic for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor; and

f) logic for initiating an event based on the results from the scanning co-processor;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data;

wherein the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria;

wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor;

wherein the scanning co-processor is capable of performing an additional scan on the additional data while scanning the data;

wherein the location of the data indicated to the scanning co-processor includes a memory location of the data stored in memory, where the memory is separate from and coupled to the scanning co-processor and the central processing unit via a bus that employs direct memory access.

34. (Currently Amended) A method for scanning data, comprising:

a) executing scanning control logic utilizing a central processing unit;

b) identifying a request related to data at the central processing unit;

c) determining whether the data meets a predetermined criteria utilizing the central processing unit under the control of the scanning control logic;

d) indicating a location of the data to a scanning co-processor coupled to the central processing unit if it is determined that the data meets the predetermined criteria;

e) collecting scanning information from additional memory on the scanning co-processor;

f) scanning the data with the scanning co-processor utilizing the scanning information under the control of the scanning control logic;

g) waiting for results from the scanning co-processor;

h) executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor;

i) queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor;

j) initiating a security event upon the receipt of unfavorable results from the scanning co-processor including a situation where malicious code is detected; and

k) processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein the criteria is based on a type of a file associated with the data;

wherein the scanning co-processor is capable of performing an additional scan on the additional data while scanning the data;

wherein the location of the data indicated to the scanning co-processor includes a memory location of the data stored in memory, where the memory is separate from and coupled to the scanning co-processor and the central processing unit via a bus that employs direct memory access.

35. (Currently Amended) A system for scanning data, comprising:

a) means for executing scanning control logic utilizing a central processing unit;

b) means for identifying a request related to data at the central processing unit;

c) means for determining whether the data meets a predetermined criteria utilizing the central processing unit under the control of the scanning control logic;

d) means for indicating a location of the data to a scanning co-processor coupled to the central processing unit if it is determined that the data meets the predetermined criteria;

e) means for collecting scanning information from additional memory on the scanning co-processor;

f) means for scanning the data with the scanning co-processor utilizing the scanning information under the control of the scanning control logic;

g) means for waiting for results from the scanning co-processor;

h) means for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor;

i) means for queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor;

j) means for initiating a security event upon the receipt of unfavorable results from the scanning co-processor including a situation where malicious code is detected; and

k) means for processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein the criteria is based on a type of a file associated with the data;

wherein the scanning co-processor is capable of performing an additional scan on the additional data while scanning the data;

wherein the location of the data indicated to the scanning co-processor includes a memory location of the data stored in memory, where the memory is separate from and coupled to the scanning co-processor and the central processing unit via a bus that employs direct memory access.

36. (Original) The system as recited in claim 35, wherein the scanning information is updated via a network periodically.

37. (Original) The system as recited in claim 35, wherein the additional logic to be executed and the additional data queued to be scanned are handled utilizing multi-threading algorithms.

38. (Previously Presented) The method as recited in claim 1, wherein the criteria is further based on a user.

39. (Previously Presented) The method as recited in claim 1, wherein the criteria is further based on software logic run by a bios.

40. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed automatically.

41. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed automatically when a computer is booted up.

42. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed manually by a user.

43. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed using software logic run by a bios.

44. (Previously Presented) The method as recited in claim 1, wherein the central processing unit aids the scanning co-processor when a large amount of data is to be scanned.